We claim:

1. A method for providing a user with access to multiple accounts using a common password which is valid for each of the multiple accounts, wherein each of the multiple accounts has associated with it a unique designated password, the method comprising:

generating a designated password which is to be associated with at least one of the user's multiple accounts;

receiving login information from the user for the at least one of the user's multiple accounts, wherein the login information includes a user ID belonging the user and the user's common password; and

determining if the user has provided valid login information based on a comparison which takes into the account the user's ID, common password and the designated password generated for the at least one of the user's multiple accounts.

2. The method of claim 1, wherein the designated password is generated by a hash function of the common password and some account-dependent information.

3. The method of claim 2, further comprising:

forming a symmetric key from the results of the hash function.

4. The method of claim 3, wherein the symmetric key is used to encrypt the random number.

5. The method of claim 4, wherein the random number is encrypted via a symmetric encryption algorithm.

6. The method of claim 1, wherein receiving login information from the user for at least one of the user's multiple accounts, wherein the login information includes a user ID and the user's common password includes:

providing at least one input facility for the user to provide the user ID and common password.

7. The method of claim 1, wherein determining if the user has provided valid login information based on a comparison which takes into the account the user's ID, common password and the designated password generated for the at least one of the user's multiple accounts includes:

performing a hash function upon the designated password; and

comparing the results of the hash function upon the designated password with a corresponding stored result to determine if a match exists.

8. The method of claim 7, further comprising:

providing access to the at least one of the user's multiple accounts if a match exists.

9. The method of claim 1, wherein determining if the user has provided valid login information based on a comparison which takes into the account the user's ID, common password and the designated password generated for the at least one of the user's multiple accounts includes:

calculating the designated password according to a password transform algorithm.

10. A method for providing access to multiple online accounts via a common password, the method comprising:

receiving a common password associated with an online account; and

determining if the universal password is valid for the associated online account based upon a designated password which was previously generated for the associated online account, wherein the designated password was previously generated based upon a password transform calculation.

11. The method of claim 8, wherein the password transform calculation is based upon a user ID for the associated online account, the universal password, a server name and a random number.

12. The method of claim 9, wherein the password transform is represented by a text conversion of the following hash function:

$$\text{Hash}(Ui + Pc + Si + Nr)$$

where Ui stands for a user ID, Pc for a common password, Si for a server name and Nr for a random number.

13. The method of claim 8, further comprising:

generating a designated password for each of the multiple online accounts which is accessible via the common password.

14. A method for providing access to multiple Web accounts via a universal password which is valid for the multiple Web accounts, the method comprising:

providing a designated password for each of the multiple Web accounts;

receiving the universal password for access to at least one of the multiple Web accounts;

determining if the universal password is valid based on the associated designated password for the at least one of the multiple Web accounts; and

providing access to the at least one of the multiple Web accounts provided the universal password is valid.

15. The method of claim 14, wherein the designated password is calculated for each of the multiple Web accounts based on a hash function which incorporates the universal password as an input to the hash function.

16. The method of claim 15, wherein the hash function also incorporates a user ID and an account server name as inputs to the hash function.

17. The method of claim 15, wherein the hash function also incorporates a random as an input to the hash function.

18. The method of claim 14, wherein determining if the universal password is valid based on the associated designated password for the at least one of the multiple Web accounts includes:

receiving a user ID;

retrieving an encrypted random number based on the user ID;

receiving the associated designated password; and

comparing the received associated designated password with a corresponding saved designated password for the at least one of the multiple Web accounts.

19. The method of claim 14, further comprising:

providing a new designated password for the at least one of the multiple Web accounts if requested.

20. The method of claim 14, wherein providing a new designated password for the at least one of the multiple Web accounts if requested includes:

generating a random number; and

calculating the new designated password based on at least the universal password and the random number.